

# ZERO REPULSION IN FAMILIES OF ELLIPTIC CURVE $L$ -FUNCTIONS AND AN OBSERVATION OF S. J. MILLER

SIMON MARSHALL

ABSTRACT. We provide a theoretical explanation for an observation of S. J. Miller that if  $L(s, E)$  is an elliptic curve  $L$ -function for which  $L(1/2, E) \neq 0$ , then the lowest lying zero of  $L(s, E)$  exhibits a repulsion from the critical point which is not explained by the standard Katz-Sarnak heuristics. We establish a similar result in the case of first-order vanishing.

## 1. INTRODUCTION

In the paper [10], S. J. Miller investigated the statistics of the zeros of various families of elliptic curve  $L$ -functions. His key observation is illustrated in Figure 1 below. It shows a histogram of the first zero above the central point for rank zero elliptic curve  $L$ -functions generated by randomly selecting the coefficients  $c_1$  up to  $c_6$  in the defining equation

$$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6$$

for curves with conductors in the ranges indicated in the caption. The zeros are scaled by the mean density of low zeros of the  $L$ -functions and the plots are normalized so that they represent the probability density function for the first zero of  $L$ -functions from this family. Miller observes that there is clear repulsion of the first zero from the central point; that is, the plots drop to zero at the origin, indicating a very low probability of finding an  $L$ -function with a low first zero. This is quite surprising, as one would expect to be able to model the distribution of the lowest zeros by the eigenvalue distribution of matrices in  $SO(2N)$ , with  $N$  chosen to be equal to half the logarithm of the conductor of the curve. However, it is well known in random matrix theory that matrices in  $SO(2N)$  exhibit no repulsion of the first eigenvalue from the origin.

In this paper, we prove a result which provides theoretical support for Miller's observation. Rather than considering algebraic families of elliptic curves, we consider quadratic twists of a fixed curve  $E/\mathbb{Q}$ . Let  $d \neq 1$  be a fundamental discriminant which is relatively prime to the conductor  $M$  of  $E$ , and let  $\chi_d$  be the associated quadratic character of modulus  $|d|$ . We shall consider the families  $\mathcal{F}^+(E)$  and  $\mathcal{F}^-(E)$  of all even and odd twists of  $E$  by the characters  $\chi_d$ , and define  $\mathcal{D}^+(E)$  and  $\mathcal{D}^-(E)$  to be the corresponding sets of fundamental discriminants. In addition, we define the subfamilies  $\mathcal{F}^0(E) \subset \mathcal{F}^+(E)$  and  $\mathcal{F}^1(E) \subset \mathcal{F}^-(E)$  by

$$\mathcal{F}^i(E) = \{L(s, E \times \chi_d) \mid \text{ord}_{s=1/2} L(s, E \times \chi_d) = i\}, \quad i = 0, 1,$$

together with the associated sets of discriminants

$$\mathcal{D}^i(E) = \{d \mid \text{ord}_{s=1/2} L(s, E \times \chi_d) = i\}.$$

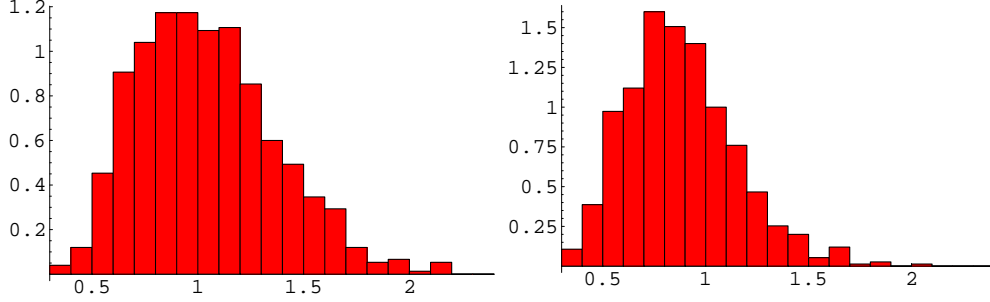


FIGURE 1. First normalized zero above the central point: Left: 750 rank 0 curves from  $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ ,  $\log(\text{cond}) \in [3.2, 12.6]$ . Right: 750 rank 0 curves from  $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ ,  $\log(\text{cond}) \in [12.6, 14.9]$ .

As is standard, we shall assume that all  $L$ -functions under consideration satisfy the Riemann hypothesis, and for any  $d$  we define  $\gamma_d$  to be the height of the lowest non-real zero of  $L(s, E \times \chi_d)$ . Our main result is the following.

**Theorem 1.** *For all  $d \in \mathcal{D}^0(E)$ , we have*

$$(1) \quad \frac{\ln |\gamma_d|}{\ln |d|} \geq -1/4 + O_{E,\epsilon}((\ln \ln |d|)^{-1+\epsilon}).$$

*In the odd case, there exists a nonzero integer  $d_0$  satisfying  $(d_0, 2M) = 1$  such that if we define*

$$\mathcal{D}_{d_0}^-(E) = \{d \mid (d, 2Md_0) = 1, d_0d < 0, d_0d \text{ is square mod } 4M\},$$

*then  $\mathcal{D}_{d_0}^-(E) \subseteq \mathcal{D}^-(E)$  and for all  $d \in \mathcal{D}^1(E) \cap \mathcal{D}_{d_0}^-(E)$  we have*

$$\frac{\ln |\gamma_d|}{\ln |d|} \geq -1/4 + O_{E,\epsilon}((\ln \ln |d|)^{-1+\epsilon}).$$

**1.1. Relation to the Katz-Sarnak heuristics.** We shall first discuss the relationship between Theorem 1 and the Katz-Sarnak heuristics in the simpler case of even functional equation. While the zero repulsion of Theorem 1 is only on a scale of  $d^{-1/4+o(1)}$ , which is very small in comparison with the mean zero spacing of  $\sim \ln |d|^{-1}$ , the fact that it holds for all members of the (conjecturally) large family  $\mathcal{F}^0(E)$  means that one can infer properties of the distribution of rescaled lowest zeros from it under some natural assumptions. Let  $D > 0$  be given, and let  $\mathcal{L}_D$  be the multiset of rescaled lowest zeros,

$$\mathcal{L}_D = \{\gamma_d \ln |d| \mid d \in \mathcal{D}^0(E), D/2 \leq |d| \leq D\}.$$

Suppose that the set  $\mathcal{L}_D$  has a limiting distribution of the form  $\rho(x)dx$  as  $D \rightarrow \infty$ , where  $\rho(x)$  is a smooth density on  $[0, \infty)$ . If  $\rho(x)$  vanishes to order  $r$  at the origin and we make the natural assumption that  $|\mathcal{L}_D| \gg D$  as  $D \rightarrow \infty$ , then we have

$$P(\exists x \in \mathcal{L}_D \mid x \leq D^{-1/(r+1)}) \geq \delta > 0$$

for  $D$  sufficiently large. Therefore, if  $\mathcal{L}_D$  has a limiting distribution of the type described for which  $r \leq 2$ , we obtain a contradiction to Theorem 1. This is evidence that any limiting distribution of  $\mathcal{L}_D$  has to vanish to order at least three at the origin, in agreement with Miller's data. Moreover, if one believes the 'minimalist conjecture' that  $\mathcal{F}^0(E)$  makes up a density one subset of  $\mathcal{F}^+(E)$ , then our result shows that the lowest zeros of the family  $\mathcal{F}^+(E)$  do not obey the standard Katz-Sarnak heuristics. For reasons which will become apparent in the course of the proof of Theorem 1, we believe that any such discrepancy should be viewed as a consequence of the special value formula

$$(2) \quad L(1/2, E \times \chi_d) = \kappa_E \frac{c_E(|d|)^2}{|d|^{1/2}}, \quad c_E(|d|) \in \mathbb{Z},$$

of Waldspurger [13], Kohnen-Zagier [9] and Baruch-Mao [2].

The tension between Miller's data and the standard  $SO(2N)$  model for even twists of a fixed elliptic curve has also been considered by Dueñez, Huynh, Keating, Miller and Snaith in [4]. They propose a modification to the  $SO(2N)$  model which they term an *excised orthogonal ensemble*, and which exhibits the observed repulsion from the critical point. Their excised ensemble is the subset of  $SO(2N)$  consisting of matrices  $g$  whose characteristic polynomial  $P(g, x)$  is not small at 1, which reflects the inequality

$$(3) \quad L(1/2, E \times \chi_d) \gg_E |d|^{-1/2}, \quad d \in \mathcal{D}^0(E)$$

that follows from the special value formula (2). We note that this gap is also the basis of our proof of Theorem 1 in the even case. The natural choice of cut-off in the excised ensemble of [4] is  $|P(g, 1)| \geq C|d|^{-1/2}$  for some constant  $C$ , and with this choice they prove that their probability distribution, denoted  $R_1^{Tx}(\theta)d\theta$ , exhibits a hard gap around the origin similar to that of Theorem 1. More precisely, they show that  $R_1^{Tx}(\theta) = 0$  for  $|\theta| \ll d^{-1/4+\delta}$  (Theorem 1.3, [4]), where  $\delta > 0$  depends on fitted parameters and may be made arbitrarily small. Moreover, it seems likely that they would have vanishing of  $R_1^{Tx}(\theta)$  for  $|\theta| \ll |d|^{-1/4+o(1)}$  under some equidistribution assumption on the zeros of the matrices in their ensemble. This is analogous to the way that obtaining an exponent of  $-1/4$  in Theorem 1 requires controlling the bulk of the zeros of  $L(s, E \times \chi_d)$ .

In the case of odd functional equation, we now define  $\mathcal{L}_D$  to be

$$\mathcal{L}_D = \{\gamma_d \ln |d| \mid d \in \mathcal{D}^1(E) \cap \mathcal{D}_{d_0}^-(E), D/2 \leq |d| \leq D\}.$$

The minimalist conjecture would again imply that  $\mathcal{D}^1(E) \cap \mathcal{D}_{d_0}^-(E)$  is a density one subsequence of  $\mathcal{D}_{d_0}^-(E)$ , and because this has  $\gg D$  elements of size at most  $D$ , we may again combine the odd case of Theorem 1 with the above argument to deduce that any smooth limiting distribution of  $\mathcal{L}_D$  must vanish to order at least three. Applying the minimalist conjecture once more, we obtain the same result for the lowest zeros in the family  $\mathcal{F}_{d_0}^-$  corresponding to  $\mathcal{D}_{d_0}^-$ . The Katz-Sarnak heuristics predict that these zeros should have the same distribution as the first nontrivial eigenvalue of a random matrix in  $SO(2N+1)$ , but this distribution only vanishes to second order at the origin (see pages 10-11 and 411-416 of [7], or

page 10 of [8]). Similarly to the even case, we shall see that this discrepancy may be viewed as a consequence of the formula of Gross-Zagier [5] for the central derivative of  $L(s, E \times \chi_d)$ , together with a lower bound for the height of a nontorsion point on an elliptic curve as in Anderson-Masser [1].

**Acknowledgements:** We would like to thank Peter Sarnak, Eduardo Dueñez, Duc Khiem Huynh, Jonathan Keating, Steven J. Miller, Nina Snaith and David Hansen for many helpful discussions, and Nicolas Templier for explaining the correct application of the Gross-Zagier formula in the odd case to us.

## 2. PROOF OF THEOREM 1 IN THE EVEN CASE

We shall first present the proof of Theorem 1 in the case of even functional equation, which combines the special value inequality (3) with a complex analytic argument. To extend the proof to the odd case, we only need to replace this inequality with an analogue for the central derivative, which may be derived from the Gross-Zagier formula and a height gap for points on elliptic curves. This is carried out in section 3.

It should be noted that if one is content to replace the error term in Theorem 1 with  $o(1)$  then the result follows immediately from the fact that the completed  $L$ -function  $\Lambda(s, E \times \chi_d)$  has vanishing central derivative, and (after suitable normalisation) its central value satisfies (3) while its second derivative on the critical line is  $\ll |d|^\epsilon$  by Lindelöf. Our refinement proceeds by combining (3) with Jensen's formula in the ball of radius 1 at the central point. Let  $\{\gamma_{d,n} | n \geq 1\}$  be the multiset of imaginary parts of zeros of  $L(s, E \times \chi_d)$  (that is, counted with multiplicity), and define  $Q = \ln \ln |d|$ . Note that all implied constants will be assumed to depend on  $E$  from now on. Jensen's formula states that

$$\begin{aligned}
 \sum_{1 \geq |\gamma_{d,n}|} \ln |\gamma_{d,n}| + \frac{1}{2\pi} \int_0^{2\pi} \ln |L(1/2 + e^{i\theta}, E \times \chi_d)| d\theta &= \ln |L(1/2, E \times \chi_d)| \\
 \sum_{Q^{-1+\epsilon} \geq |\gamma_{d,n}|} \ln |\gamma_{d,n}| + \sum_{1 \geq |\gamma_{d,n}| \geq Q^{-1+\epsilon}} \ln |\gamma_{d,n}| \\
 + \frac{1}{2\pi} \int_0^{2\pi} \ln |L(1/2 + e^{i\theta}, E \times \chi_d)| d\theta &\geq -1/2 \ln |d| + O(1),
 \end{aligned}
 \tag{4}$$

where we have broken up the sum on the LHS of (4) with the aid of an arbitrarily chosen parameter  $\epsilon$  satisfying  $1 > \epsilon > 0$ . We shall prove the following asymptotics for the last two terms on the LHS of (4):

**Proposition 2.** *For every  $1 > \epsilon > 0$ , the second term in (4) satisfies the asymptotic*

$$\sum_{1 \geq |\gamma_{d,n}| \geq Q^{-1+\epsilon}} \ln |\gamma_{d,n}| = -\frac{2}{\pi} \ln |d| + O_\epsilon(\ln |d| Q^{-1+\epsilon}).
 \tag{5}$$

**Proposition 3.** *For every  $1 > \epsilon > 0$ , the third term in (4) satisfies the bound*

$$\frac{1}{2\pi} \int_0^{2\pi} \ln |L(1/2 + e^{i\theta}, E \times \chi_d)| d\theta \leq \frac{2}{\pi} \ln |d| + O_\epsilon(\ln |d| Q^{-1+\epsilon}).
 \tag{6}$$

After substituting the asymptotics of Propositions 2 and 3 into equation (4), we have

$$\sum_{Q^{-1+\epsilon} \leq |\gamma_{d,n}|} \ln |\gamma_{d,n}| \geq -1/2 \ln |d| + O_\epsilon(\ln |d| Q^{-1+\epsilon}) + O(1),$$

and Theorem 1 follows from this on throwing away all but the lowest pair of conjugate zeros in the sum.

**2.1. Estimating sums over zeros.** Proposition 2 will follow by integration by parts from the following estimate for the counting function  $N_d(a, b)$ , defined by

$$N_d(a, b) = |\{\gamma_{d,n} | a \leq \gamma_{d,n} \leq b\}|.$$

**Lemma 4.** *We have the asymptotic*

$$(7) \quad N_d(a, b) = \frac{(b-a) \ln |d|}{\pi} + O_\epsilon(\ln |d| Q^{-1+\epsilon})$$

*uniformly for  $a$  and  $b$  in any compact interval.*

Lemma 4 will be proven in turn by applying the explicit formula of the  $L$ -function  $L(s, E \times \chi_d)$ . The particular form that we shall use is the one stated in Proposition 2.1 of [12]. To recall it, let  $g \in C_0^\infty(\mathbb{R})$  be given, and define  $h(r) = \int_{-\infty}^{\infty} g(x) e^{irx} dx$ . Let the conductor of  $L(s, E)$  be  $M$ . If we have

$$L(s, E) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s},$$

we define  $c_d(n) = \Lambda(n) \chi_d(n) a(n)$  so that

$$-\frac{L'}{L}(s, E \times \chi_d) = \sum_{n=1}^{\infty} \frac{c_d(n)}{n^s}.$$

With these notations, the explicit formula may be stated as follows:

**Proposition 5 (The explicit formula).** *The zeros  $\{\gamma_{d,n}\}$  and coefficients  $c_d(n)$  satisfy the relation*

$$(8) \quad \sum_{\gamma_{d,n}} h(\gamma_{d,n}) = \frac{1}{2\pi} \int_{-\infty}^{\infty} h(r) \left( \ln(Md^2) - 2 \ln 2\pi + \frac{\Gamma'}{\Gamma}(1+ir) + \frac{\Gamma'}{\Gamma}(1-ir) \right) dr \\ - \sum_{n=1}^{\infty} \left( \frac{c_d(n)}{\sqrt{n}} g(\ln n) + \frac{\overline{c_d(n)}}{\sqrt{n}} g(-\ln n) \right).$$

We shall first use the explicit formula to prove a smooth version of Lemma 4. To state it, let  $f_0 \in C_0^\infty(\mathbb{R})$  be a real even function with support in  $[-1/2, 1/2]$ , and define  $f = f_0 * f_0$ . We then define

$$f_Q(x) = f(x/Q), \quad \widehat{f}(r) = \int_{-\infty}^{\infty} f(x) e^{irx} dx, \quad \widehat{f_Q}(r) = \int_{-\infty}^{\infty} f_Q(x) e^{irx} dx.$$

Our construction of  $f$  implies that  $\widehat{f}(r) \geq 0$ , and we may normalise  $f$  so that  $\int \widehat{f}(r)dr = 1$ . Let  $I(r)$  be the characteristic function of the interval  $[a, b]$ , and define  $I_Q$  to be the smooth approximation  $I * \widehat{f_Q}$  to  $I$ . We then have

**Lemma 6.** *We have the asymptotic*

$$\sum_{\gamma_{d,n}} I_Q(\gamma_{d,n}) = \frac{(b-a) \ln |d|}{\pi} + O(\ln |d|^{2/3}),$$

uniformly for  $a$  and  $b$  in any compact interval.

*Proof.* Define  $g_Q$  to be the function

$$\begin{aligned} g_Q(x) &= f_Q(x) \frac{-1}{2\pi} \int_a^b e^{-itx} dt \\ &= \frac{1}{2\pi ix} (e^{-ibx} - e^{-iax}) f_Q(x), \end{aligned}$$

so that  $I_Q = \widehat{g_Q}$ . Substituting the pair  $g_Q, I_Q$  into the explicit formula yields

$$\begin{aligned} (9) \quad \sum_{\gamma_{d,n}} I_Q(\gamma_{d,n}) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} I_Q(r) \left( \ln(Md^2) - 2 \ln 2\pi + \frac{\Gamma'}{\Gamma}(1+ir) + \frac{\Gamma'}{\Gamma}(1-ir) \right) dr \\ &\quad - \sum_{n=1}^{\infty} \left( \frac{c_d(n)}{\sqrt{n}} g_Q(\ln n) + \frac{\overline{c_d(n)}}{\sqrt{n}} g_Q(-\ln n) \right). \end{aligned}$$

Because  $I_Q(r)$  has rapid decay in  $r$  at a rate which is uniform as  $Q \rightarrow \infty$ , and  $\int_{-\infty}^{\infty} I_Q(r)dr = (b-a)$ , we may simplify the integral in (9) so that it becomes

$$(10) \quad \sum_{\gamma_{d,n}} I_Q(\gamma_{d,n}) = \frac{(b-a) \ln |d|}{\pi} + O(1) - \sum_{n=1}^{\infty} \left( \frac{c_d(n)}{\sqrt{n}} g_Q(\ln n) + \frac{\overline{c_d(n)}}{\sqrt{n}} g_Q(-\ln n) \right).$$

We may bound the sum in (10) using the following properties of  $g_Q$ :

$$\begin{aligned} \text{supp}(g_Q) &\subseteq [-Q, Q], \\ |g_Q(x)| &\ll |f_Q(x)| \left| \int_a^b e^{-itx} dt \right| \\ &\ll |a-b| \ll 1. \end{aligned}$$

With these, we have

$$\begin{aligned}
(11) \quad \left| \sum_{n=1}^{\infty} \frac{c_d(n)}{\sqrt{n}} g_Q(\ln n) \right| &\leq \sum_{n=1}^{e^Q} \frac{|c_d(n)|}{\sqrt{n}} \\
&\ll_{\epsilon} \sum_{n=1}^{e^Q} n^{-1/2+\epsilon} \\
&\ll_{\epsilon} e^{(1/2+\epsilon)Q} \\
&= \ln |d|^{(1/2+\epsilon)},
\end{aligned}$$

and likewise for the second term. Note that we have used the fact that the coefficients  $a(n)$  satisfy the Ramanujan bound  $|a(n)| \ll n^{\epsilon}$ , which implies the same bound for  $|c_d(n)|$ . Substituting (11) into (10) and relaxing  $1/2 + \epsilon$  to  $2/3$  gives the result.  $\square$

We now deduce Lemma 4 from Lemma 6 by comparing  $I_Q$  with  $I$ . If  $r$  lies outside the intervals  $[a - Q^{-1+\epsilon}, a + Q^{-1+\epsilon}]$  and  $[b - Q^{-1+\epsilon}, b + Q^{-1+\epsilon}]$ , the difference  $|I(r) - I_Q(r)|$  may be estimated as

$$\begin{aligned}
(12) \quad |I(r) - I_Q(r)| &\leq \left| \left( \int_{-\infty}^{-Q^{-1+\epsilon}} + \int_{Q^{-1+\epsilon}}^{\infty} \right) \widehat{f}_Q(r) dr \right| \\
&= \left| \left( \int_{-\infty}^{-Q^{-1+\epsilon}} + \int_{Q^{-1+\epsilon}}^{\infty} \right) Q \widehat{f}(Qr) dr \right| \\
&= \left| \left( \int_{-\infty}^{-Q^{\epsilon}} + \int_{Q^{\epsilon}}^{\infty} \right) \widehat{f}(r) dr \right| \\
&\ll_{\epsilon, A} Q^{-A}
\end{aligned}$$

for any  $A$ , by the rapid decay of  $\widehat{f}$ . The positivity of  $I_Q$  means that we may estimate the sum  $\sum I_Q(\gamma_{d,n})$  from below by its restriction to  $\gamma_{d,n} \in [a + Q^{-1+\epsilon}, b - Q^{-1+\epsilon}]$ , after which we may apply (12) and Lemma 6 to bound  $N_d(a, b)$  from above as follows:

$$\begin{aligned}
\sum_{\gamma_{d,n}} I_Q(\gamma_{d,n}) &\geq \sum_{b - Q^{-1+\epsilon} \leq \gamma_{d,n} \leq a + Q^{-1+\epsilon}} I_Q(\gamma_{d,n}) \\
\frac{(b-a) \ln |d|}{\pi} + O(\ln |d|^{2/3}) &\geq (1 + O_{\epsilon}(Q^{-2})) N_d(a + Q^{-1+\epsilon}, b - Q^{-1+\epsilon}).
\end{aligned}$$

Replacing  $a$  and  $b$  with  $a - Q^{-1+\epsilon}$  and  $b + Q^{-1+\epsilon}$  yields the upper bound in Lemma 4.

We derive a lower bound for  $N_d(a, b)$  in a similar way, starting from the inequality

$$\begin{aligned}
(1 + O_\epsilon(Q^{-2}))N_d(a - Q^{-1+\epsilon}, b + Q^{-1+\epsilon}) &\geq \sum_{b+Q^{-1+\epsilon} \geq \gamma_{d,n} \geq a-Q^{-1+\epsilon}} I_Q(\gamma_{d,n}) \\
&= \frac{(b-a) \ln |d|}{\pi} + O(\ln |d|^{2/3}) \\
&\quad - \sum_{\gamma_{d,n} \notin (a-Q^{-1+\epsilon}, b+Q^{-1+\epsilon})} I_Q(\gamma_{d,n})
\end{aligned}$$

The bounds

$$|I_Q(r)| \ll_{\epsilon, A} (Qr)^{-A}, \quad r \notin (a - Q^{-1+\epsilon}, b + Q^{-1+\epsilon})$$

and  $N_d(-T, T) \ll \ln |d| T \ln T$  for  $T \geq 1$  (see for instance Theorem 5.8, V, p. 104 [6]) imply that

$$\sum_{\gamma_{d,n} \notin (a-Q^{-1+\epsilon}, b+Q^{-1+\epsilon})} |I_Q(\gamma_{d,n})| \ll_\epsilon \ln |d| Q^{-2},$$

and so

$$N_d(a - Q^{-1+\epsilon}, b + Q^{-1+\epsilon}) \geq \frac{(b-a) \ln |d|}{\pi} + O(\ln |d| Q^{-2}).$$

The lower bound in Lemma 4 again follows from this by substitution.

It remains to derive Proposition 2 from Lemma 4. We first apply integration by parts, which gives

$$\begin{aligned}
\sum_{1 \geq \gamma_{d,n} \geq Q^{-1+\epsilon}} \ln \gamma_{d,n} &= N_d(0, x) \ln x \Big|_{Q^{-1+\epsilon}}^1 - \int_{Q^{-1+\epsilon}}^1 N_d(0, x) \frac{dx}{x} \\
&= -N_d(0, Q^{-1+\epsilon}) \ln Q^{-1+\epsilon} - \int_{Q^{-1+\epsilon}}^1 N_d(0, x) \frac{dx}{x}.
\end{aligned}$$

After substituting the asymptotic of Lemma 4, this becomes

$$\begin{aligned}
\sum_{1 \geq \gamma_{d,n} \geq Q^{-1+\epsilon}} \ln \gamma_{d,n} &= O_\epsilon(\ln |d| Q^{-1+\epsilon} \ln Q) - \int_{Q^{-1+\epsilon}}^1 \left( \frac{x}{\pi} \ln |d| + O_\epsilon(\ln |d| Q^{-1+\epsilon}) \right) \frac{dx}{x} \\
&= -(1 - Q^{-1+\epsilon}) \frac{\ln |d|}{\pi} + O_\epsilon(\ln |d| Q^{-1+\epsilon} \ln Q) \\
&= -\frac{\ln |d|}{\pi} + O_\epsilon(\ln |d| Q^{-1+\epsilon}),
\end{aligned}$$

and Proposition 2 follows from this by the symmetry of  $\{\gamma_{d,n}\}$ .



**2.2. Proof of Proposition 3.** We shall prove Proposition 3 with the aid of the following explicit subconvex bound for  $L(s, E \times \chi_d)$  (Theorem 5.19, V, p. 116 [6]), which is valid for any  $L$ -function satisfying Riemann and Ramanujan.

**Proposition 7.** *We have the bound*

$$(13) \quad \ln |L(s, E \times \chi_d)| \ll \frac{(\ln |d|)^{2-2\sigma}}{(2\sigma-1)Q} + Q$$

for all  $s$  satisfying  $|s - 1/2| \leq 1$ .

We divide the integral in Proposition 3 into three regions, the first containing the points within  $Q^{-1+\epsilon}$  of the critical line, and the second and third the semicircles to the right and left of the critical line. In the first region, the length of the arc of integration and the convex estimate  $\ln |L(s, E \times \chi_d)| \ll \ln |d|$  imply that the integral is  $\ll \ln |d| Q^{-1+\epsilon}$ . In the right semicircle, we apply Proposition 7 and the bound  $\sigma - 1/2 \geq Q^{-1+\epsilon}$  to obtain

$$(14) \quad \begin{aligned} \ln |L(s, E \times \chi_d)| &\ll \frac{(\ln |d|)^{1-2Q^{-1+\epsilon}}}{Q^{-1+\epsilon}Q} + Q \\ &= \ln |d| \exp(-2Q^{-1+\epsilon} \ln \ln |d|) Q^{-\epsilon} + Q \\ &= \ln |d| \exp(-2Q^\epsilon) Q^{-\epsilon} + Q \\ &\ll_\epsilon \ln |d| Q^{-1}. \end{aligned}$$

This implies that the integral over the right semicircle is also  $O_\epsilon(\ln |d| Q^{-1})$ . In the left semicircle, we combine (14) with the functional equation to see that

$$(15) \quad \ln |L(s, E \times \chi_d)| \leq (1 - 2\sigma) \ln |d| + O_\epsilon(\ln |d| Q^{-1}).$$

This implies that the integral over the left semicircle is  $\leq 2 \ln |d| / \pi + O_\epsilon(\ln |d| Q^{-1})$ , which completes the proof.

### 3. THE PROOF IN THE ODD CASE

We begin the proof of Theorem 1 in the case of odd functional equation by applying the results of Bump-Friedberg-Hoffstein [3], Murty-Murty [11], and Waldspurger [14, 15] to deduce the existence of a quadratic character  $\chi_{d_0}$  with  $(2M, d_0) = 1$  such that  $L(1/2, E \times \chi_{d_0}) \neq 0$ . This is the  $d_0$  that we shall take in the statement of Theorem 1. If we choose a second fundamental discriminant  $d$  satisfying

$$(d, 2Md_0) = 1, \quad d_0 d < 0, \quad d_0 d \equiv \square(4M),$$

then the discussion on pages 268-269 of [5] shows that  $L(s, E \times \chi_d)$  has odd functional equation and hence  $\mathcal{D}_{d_0}^-(E) \subseteq \mathcal{D}^-(E)$  as claimed. We may deduce Theorem 1 from the following lemma in exactly the same manner as in the case of even functional equation, by applying Jensen's formula to  $L(s, E \times \chi_d)/(s - 1/2)$ .

**Lemma 8.** *For  $d \in \mathcal{D}^1(E) \cap \mathcal{D}_{d_0}^-(E)$ , we have*

$$L'(1/2, E \times \chi_d) \gg |d|^{-1/2}.$$

*Proof.* The conditions that  $(d, d_0) = 1$  and  $d_0 d < 0$  allow us to define a genus class character  $\chi_{d,d_0}$  of the imaginary quadratic field  $K = \mathbb{Q}(\sqrt{d_0 d})$  (see for instance [6], chapter 22, page 510). We base-change  $E$  to  $K$  and twist by  $\chi_{d,d_0}$ , and denote the associated  $L$ -function by  $L(s, E_K \times \chi_{d,d_0})$ . As the discriminant of  $K$  is prime to  $2M$  and all primes dividing  $M$  split in  $K$ , we may apply the Gross-Zagier formula [5] to the central derivative  $L'(1/2, E_K \times \chi_{d,d_0})$  to obtain

$$(16) \quad L'(1/2, E_K \times \chi_{d,d_0}) = C_E h(P_{d,d_0}) |d_0 d|^{-1/2}.$$

Here,  $P_{d,d_0}$  is an algebraic point on  $E$  which is defined over  $\mathbb{Q}(\sqrt{d})$  (see the discussion on pages 268-269 of [5]), and  $h(\cdot)$  denotes the canonical height on  $E$ . The Kronecker factorisation formula and the fact that  $L(1/2, E \times \chi_d) = 0$  imply that

$$\begin{aligned} L(s, E_K \times \chi_{d,d_0}) &= L(s, E \times \chi_{d_0}) L(s, E \times \chi_d) \\ L'(1/2, E_K \times \chi_{d,d_0}) &= L(1/2, E \times \chi_{d_0}) L'(1/2, E \times \chi_d). \end{aligned}$$

Substituting this into (16) and using our assumption that  $L(1/2, E \times \chi_{d_0}) \neq 0$ , we have

$$L'(1/2, E \times \chi_d) = C_{E,d_0} h(P_{d,d_0}) |d|^{-1/2}.$$

We now apply the results of Anderson-Masser [1], which state that if  $P$  is a nontorsion algebraic point on  $E$  whose degree over  $\mathbb{Q}$  is bounded, then the height  $h(P)$  must be bounded from below. Our assumption that  $L'(1/2, E \times \chi_d) \neq 0$  implies that  $P_{d,d_0}$  is not torsion, from which we then deduce that

$$L'(1/2, E \times \chi_d) \gg |d|^{-1/2}$$

as required. □

## REFERENCES

- [1] M. Anderson, D. Masser: *Lower bounds for heights on elliptic curves*, Math. Zeit. **174** no. 1 (1980), 23-34.
- [2] E. M. Baruch, Z. Mao: *Central value of automorphic  $L$ -functions*, Geom. Funct. Anal. **17** (2007), 333-384.
- [3] D. Bump, S. Freidberg, J. Hoffstein: *Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic  $L$ -functions and their derivatives*, Ann. of Math. **131** no. 1 (1990), 53-127.
- [4] E. Dueñez, D. K. Huynh, J. P. Keating, S. J. Miller, N. C. Snaith: *A random matrix model for elliptic curve  $L$ -functions of finite conductor*, preprint, available as arXiv:1107.4426v2.
- [5] B. Gross, D. Zagier: *Heegner points and derivatives of  $L$ -series*, Invent. Math. **84** no. 2 (1986), 225-320.
- [6] H. Iwaniec, E. Kowalski: *Analytic Number Theory*, American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004. xii + 615 pp.
- [7] N. Katz, P. Sarnak: *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications **45**, AMS, Providence, 1999.
- [8] N. Katz, P. Sarnak: *Zeros of zeta functions and symmetries*, Bull. AMS **36** (1999), 1-26.
- [9] W. Kohnen, D. Zagier: *Values of  $L$ -series of modular forms at the center of the critical strip*, Invent. Math. **64** (1981), 175-198.
- [10] S. Miller: *Investigations of zeros near the central point of elliptic curve  $L$ -functions*, Experiment. Math. **15** vol. 3 (2006), 257-279.
- [11] M. R. Murty, V. K. Murty: *Non-vanishing of  $L$ -functions and applications*, Birkhäuser, 1997.

- [12] Z. Rudnick, P. Sarnak: *Zeros of principal L-functions and random matrix theory*, Duke Math. J. **81** no. 2 (1996), 269-322.
- [13] J. L. Waldspurger: *Correspondences de Shimura et Shintani*, J. Math. Pures et Appl. **59** (1980), 1-133.
- [14] J. L. Waldspurger: *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.
- [15] J. L. Waldspurger: *Correspondances de Shimura et quaternions*, Forum Math. **3** (1991), 219-307.

DEPARTMENT OF MATHEMATICS, NORTHWESTERN UNIVERSITY, 2033 SHERIDAN ROAD, EVANSTON, IL 60202, USA

*E-mail address:* `slm@math.northwestern.edu`